

Defect Details

Defect Id: 203

Project: Gallery Server Pro

Name: Cross-site scripting vulnerability

Date Found: 5/21/2009

Build #: 2.3.3421

Severity: Critical

Date Fixed: 5/27/2009

Build # of Fix: 2.3.3434

Status: Closed

Estimated Work: 2 hrs

Assigned To: Roger Martin

Priority: High

Actual Work: 24 hrs

Reported By: Roger Martin

Percent Complete: 100

Description

The external media object feature allows users to upload HTML fragments such as YouTube videos. The HTML fragment is not filtered for malicious HTML tags or javascript. A user can enter specially crafted code that sends the user's cookie to a remote web site each time the external media object is viewed. This allows the malicious user to engage in session hijacking. There are other attack paths possible, such as using specially crafted text that exploits unpatched browser vulnerabilities.

The lack of filtering on external media objects was an intentional feature, and it was assumed the administrator would only give trusted users the ability to add them. However, this assumption is not always correct. Furthermore, with the release of community galleries (aka user albums) and self-registration in 2.3, a wider variety of users now have the possibility to add external media objects.

Resolution

The fix was to filter the HTML entered by a user for an external media object on the Add objects page. If the HTML contains tags, attributes, or javascript that are not authorized, the object is not added and the user is informed of the violating tags.

Rather than hard-coding the list of authorized tags and attributes as was done in previous versions, these were refactored to galleryserverpro.config. Three new settings were created:

```
allowUserEnteredJavascript (default="false")
allowedHtmlTags
allowedHtmlAttributes
```

When allowUserEnteredJavascript is false, the <script> tag is not allowed, nor is the string "javascript:". Note that it is extremely difficult to prevent javascript with 100% certainty. Consider this HTML:

```
<p onclick="alert('hi');">Click me</p>
```

In this example there are no obvious javascript indicators. This attack scenario is prevented, however, by not including onclick in the list of allowed HTML attributes.

To facilitate this change, the original code in HtmlScrubber was scrapped and a new class HtmlValidator was created. Instead of traversing the text character by character, it uses compiled regular expressions to analyze the input.

Also as part of this bug fix I modified

GalleryServerPro.Business.Metadata.MediaObjectMetadataExtractor.GetGalleryObjectMetadataItemCollection() to call the function RemoveInvalidHtmlAndScripts after extracting the metadata from an image:

```
private static void RemoveInvalidHtmlAndScripts(IEnumerable<IGalleryObjectMetadataItem> metadataItems)
```

Defect Details

```
{
foreach (IGalleryObjectMetadataItem metadataItem in metadataItems)
{
metadataItem.Value = HtmlValidator.Clean(metadataItem.Value);
}
}
```

Previously, invalid HTML in titles and captions was stored in the database encoded. This behavior has changed so that now invalid HTML is removed before being saved to the database.

The three new settings are exposed in the Site Admin area on the User Settings page.

Defect Id: 204

Project: Gallery Server Pro

Name: Error when album owner template role has albums assigned to it

Date Found: 5/27/2009

Build #: 2.3.3421

Severity: Medium Impact

Date Fixed: 5/27/2009

Build # of Fix: 2.3.3434

Status: Closed

Estimated Work: 1 hrs

Assigned To: Roger Martin

Priority: Medium

Actual Work: 1 hrs

Reported By: Roger Martin

Percent Complete: 100

Description

When the album owner template role (named `_Album Owner Template`) has been assigned to one or more albums, the following error may occur when a user logs in:

Exception Type: GalleryServerPro.ErrorHandler.CustomExceptions.BusinessException

Message:

Invalid state of GalleryServerRole instance: The AllAlbumIds property has a count of zero but the RootAlbumIds has a count greater than zero. The count of AllAlbumIds must be equal to or greater than the count of RootAlbumIds. This situation can happen if the RootAlbumIds property is modified and not persisted to the data store. Calling the Save() method will automatically cause the AllAlbumIds property to be reloaded from the data store.

Source: GalleryServerPro.Business

Target Site: GalleryServerPro.Business.Interfaces.IIntegerCollection get_AllAlbumIds()

Stack Trace:

```
at GalleryServerPro.Business.GalleryServerRole.get_AllAlbumIds()
at GalleryServerPro.Business.GalleryServerRole.Copy()
at GalleryServerPro.Web.Controller.RoleController.CreateAlbumOwnerRole(IAlbum album)
at GalleryServerPro.Web.Controller.RoleController.ValidateRoleExistsForAlbumOwner(IAlbum album)
at GalleryServerPro.Web.Controller.GalleryObjectController.SaveGalleryObject(IGalleryObject galleryObject, String username)
at GalleryServerPro.Web.Controller.AlbumController.CreateUserAlbum(String username)
at GalleryServerPro.Web.Controller.UserController.ValidateUserAlbum(String userName)
at GalleryServerPro.Web.Controls.login.Login1_LoggedIn(Object sender, EventArgs e)
at System.Web.UI.WebControls.Login.OnLoggedIn(EventArgs e)
at System.Web.UI.WebControls.Login.AttemptLogin()
```

Defect Details

```
at System.Web.UI.WebControls.Login.OnBubbleEvent(Object source, EventArgs e)
at System.Web.UI.Control.RaiseBubbleEvent(Object source, EventArgs args)
at System.Web.UI.WebControls.Button.OnCommand(CommandEventArgs e)
at System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument)
at System.Web.UI.WebControls.Button.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument)
at System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument)
at System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData)
at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)
```

Resolution

The code assumed the template role would never be assigned to an album. However, an administrator might want to do this. In this case, the code should include previously assigned albums when copying the role and creating a new one for the user album.

Part of the fix was to change the order in which album IDs are assigned to the newly copied role within `GalleryServerRole.Copy()`. Instead of this:

```
role.RootAlbumIds.AddRange(RootAlbumIds);
role.AllAlbumIds.AddRange(AllAlbumIds);
```

It was changed to:

```
role.AllAlbumIds.AddRange(AllAlbumIds);
role.RootAlbumIds.AddRange(RootAlbumIds);
```

There were also a couple minor changes to `RoleController.CreateAlbumOwnerRole`.

During the investigation of this bug I noticed some incorrect behavior during the role saving routine. Each of the data providers (SQLite and SQL Server) calls a function `ReloadAllAlbumIds` as the last step of the save. This function pulls the latest list of album IDs included in the current role from the database. It assumes the current list of album IDs (property `AllAlbumIds`) is empty, and it probably was in all cases before version 2.3. But this is not true when an album is created in `RoleController.CreateAlbumOwnerRole`. The providers were modified so that the `AllAlbumIds` property was emptied just before being refilled. Because validation logic in the `AllAlbumIds` getter throws an exception when `AllAlbumIds` is empty but `RootAlbumIds` is not (which is what happens when saving roles in the Manage roles page), I had to create a new method `ClearAllAlbumIds`.

Defect Id: 205

Project: Gallery Server Pro

Name: HTML may appear in page title

Date Found: 5/27/2009

Build #: 2.3.3421

Severity: Low Impact

Date Fixed: 5/27/2009

Build # of Fix: 2.3.3434

Status: Closed

Estimated Work: 1 hrs

Assigned To: Roger Martin

Priority: Low

Actual Work: 30 min

Reported By: Roger Martin

Percent Complete: 100

Description

The title of an album is often used in the `<title>` tag of a gallery web page. If the option to enter HTML is enabled,

Defect Details

and the user has entered HTML in an album title, that HTML can appear in the title. Browsers will often display this title in the tab and taskbar icon.

HTML should be removed the album's title when assigning it to the <title> tag.

Resolution

Modified the property PageTitle in class Website\CodeFiles\GalleryPage.cs from this:

```
public virtual string PageTitle
{
    get
    {
        if (String.IsNullOrEmpty(_pageTitle))
            return String.Concat(Resources.GalleryServerPro.UC_ThumbnailView_Album_Title_Prefix_Text, " ",
Util.TruncateTextForWeb(GetAlbum().Title, 50));
        else
            return _pageTitle;
    }
    set
    {
        this._pageTitle = value;
    }
}
```

To this:

```
public virtual string PageTitle
{
    get
    {
        if (String.IsNullOrEmpty(_pageTitle))
        {
            // Get an HTML-cleaned version of the current album's title, limited to the first 50 characters.
            string title = Util.RemoveHtmlTags(GetAlbum().Title);
            title = title.Substring(0, title.Length < 50 ? title.Length : 50);

            return String.Concat(Resources.GalleryServerPro.UC_ThumbnailView_Album_Title_Prefix_Text, " ", title);
        }
        else
            return _pageTitle;
    }
    set
    {
        this._pageTitle = value;
    }
}
```

Defect Details

Defect Id: 206

Project: Gallery Server Pro

Name: SQL Server install or upgrade script fails when database user has a default schema other than dbo

Date Found: 5/16/2009

Build #: 2.3.3421

Severity: High Impact

Date Fixed: 5/27/2009

Build # of Fix: 2.3.3434

Status: Closed

Estimated Work: 1 hrs

Assigned To: Roger Martin

Priority: High

Actual Work: 1 hrs

Reported By: Roger Martin

Percent Complete: 100

Description

When installing GSP to a SQL Server database or upgrading an existing installation that uses SQL Server, the following error may occur:

Cannot find the object "dbo.gs_AppError" because it does not exist or you do not have permissions.

```
Error executing SQL: /***** Object: Non-clustered index [dbo].[gs_AppError].[IDX_gs_AppError_FKGalleryId]
*****/ IF NOT EXISTS (SELECT * FROM sys.indexes WHERE object_id = OBJECT_ID(N'[dbo].[gs_AppError]') AND name = N'IDX_gs_AppError_FKGalleryId') CREATE NONCLUSTERED INDEX [IDX_gs_AppError_FKGalleryId] ON [dbo].[gs_AppError] ([FKGalleryId] ASC ) WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF, ONLINE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON)
```

```
Call stack: at System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection) at
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection) at
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj) at
System.Data.SqlClient.TdsParser.Run(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj) at
System.Data.SqlClient.SqlCommand.RunExecuteNonQueryTds(String methodName, Boolean async) at
System.Data.SqlClient.SqlCommand.InternalExecuteNonQuery(DbAsyncResult result, String methodName, Boolean sendToPipe) at System.Data.SqlClient.SqlCommand.ExecuteNonQuery() at
GalleryServerPro.Web.gs.pages.install.ExecuteSqlInStream(Stream stream) at
GalleryServerPro.Web.gs.pages.install.ExecuteSqlInFile(String pathToSqlFile) at
GalleryServerPro.Web.gs.pages.install.ConfigureGalleryServerSchemaForSqlServer() at
GalleryServerPro.Web.gs.pages.install.ExecuteSqlServerInstallation() at
GalleryServerPro.Web.gs.pages.install.ExecuteInstallation() at
GalleryServerPro.Web.gs.pages.install.ShowNextPanel()
```

Resolution

This occurred because the CREATE TABLE script was missing the "dbo" owner prefix. It was changed from this:

```
CREATE TABLE [gs_AppError] (...)
```

To this:

```
CREATE TABLE [dbo].[gs_AppError] (...)
```

The following files were updated:

Defect Details

Website\gs\pages\installer\sql\InstallGalleryServerProSql2000.sql
Website\gs\pages\installer\sql\InstallGalleryServerProSql2005.sql
TIS.GSP.Data.SqlServer\SqlUpgrade_2_1_3162_to_2_3_3421_SqlServer2000.sql
TIS.GSP.Data.SqlServer\SqlUpgrade_2_1_3162_to_2_3_3421_SqlServer2005.sql

Defect Id: 207

Project: Gallery Server Pro

Name: Error in cultures that use a comma instead of decimal point

Date Found: 5/16/2009

Build #: 2.3.3421

Severity: High Impact

Date Fixed: 5/27/2009

Build # of Fix: 2.3.3434

Status: Closed

Estimated Work: 1 hrs

Assigned To: Roger Martin

Priority: High

Actual Work: 1 hrs

Reported By: Roger Martin

Percent Complete: 100

Description

Two errors can occur when GSP is installed on a server with a culture that uses a comma to separate whole numbers from their fractional component

1. GSP fails with the following error when viewing the Media objects page in the Site Admin area:

Error: The value '.000001' of the MinimumValue property of 'rvTransDuration' cannot be converted to type 'Double'.

2. After any change that causes galleryserverpro.config to be updated (which is typically any edit of a page in the Site Admin area), the following error may occur:

"The value of the property 'mediaObjectTransitionDuration' cannot be parsed. The error is: 0,2 is not a valid value for Single."

Resolution

1. Added **CultureInvariantValues="true"** to gs\pages\admin\mediaobjects.ascx:

```
<asp:RangeValidator ID="rvTransDuration" runat="server" Display="Dynamic"  
ControlToValidate="txtTransDuration" Type="Double" MinimumValue=".000001"  
MaximumValue="2147483647" CultureInvariantValues="true" Text="<%"$ Resources:GalleryServerPro,  
Validation_Positive_Double_Text %>" />
```

2. Modified GalleryServerPro.Web.Controller.GspConfigController so that culture invariant versions of data types were being stored in galleryserverpro.config. For example, in the function SaveCore, the following line:

```
string attValue = field.GetValue(core).ToString();
```

was changed to this:

```
stringattValue = Convert.ToString(field.GetValue(core),  
System.Globalization.CultureInfo.InvariantCulture);
```

Defect Details

Defect Id: 208

Project: Gallery Server Pro

Name: The search page shows only the top album in the breadcrumb menu, not the current album the user

Date Found: 5/27/2009

Build #: 2.3.3421

Severity: Medium Impact

Date Fixed: 5/27/2009

Build # of Fix: 2.3.3434

Status: Closed

Estimated Work: 30 min

Assigned To: Roger Martin

Priority: Low

Actual Work: 30 min

Reported By: Roger Martin

Percent Complete: 100

Description

Navigating to the search page causes the album breadcrumb menu to show only the top album, not the current album the user may have been viewing. The only way for a user to view the previous album is to use the browser's back button. It would be better if the breadcrumb menu remembered the current album the user was viewing.

Resolution

Changed the following line of code in the event handler btnSearch_Click in gs\controls\search from this:
`Util.Redirect(PageId.search, String.Concat("search=", Util.UrlEncode(txtSearch.Text)));`

to this:

`Util.Redirect(PageId.search, String.Format("aid={0}&search={1}", this.GalleryPage.GetAlbum().Id, Util.UrlEncode(txtSearch.Text)));`

Defect Id: 209

Project: Gallery Server Pro

Name: Scroll position lost when paging on Manage Users page

Date Found: 5/29/2009

Build #: 2.3.3421

Severity: Low Impact

Date Fixed: 5/29/2009

Build # of Fix: 2.3.3436

Status: Closed

Estimated Work: 30 min

Assigned To: Roger Martin

Priority: Low

Actual Work: 30 min

Reported By: Roger Martin

Percent Complete: 100

Description

Each time you navigate to a new page of users on the Manage Users page, the focus is applied to the search text box at the top of the grid, forcing the page to scroll to the top. The page should not lose its scroll position.

Resolution

The fix was to set the AutoFocusSearchBox property on the Grid to false when the number of users exceeds the grid's page size. This code was added to the ConfigureControls function in Website\gs\pages\admin\manageusers.ascx.cs:

```
if (UserController.GetUserNames().Rows.Count > gdUsers.PageSize)
    gdUsers.AutoFocusSearchBox = false;
```

Defect Details

Defect Id: 210

Project: Gallery Server Pro

Name: Trying to create three or more users in a row does not work

Date Found: 5/29/2009

Build #: 2.3.3421

Severity: Medium Impact

Date Fixed: 5/29/2009

Build # of Fix: 2.3.3436

Status: Closed

Estimated Work: 1 hrs

Assigned To: Roger Martin

Priority: Low

Actual Work: 1 hrs

Reported By: Roger Martin

Percent Complete: 100

Description

After completing the Add User Wizard on the Manage Users page, there is a hyperlink named Create another user. When clicked, the page is reloaded with the query string parameter "action=add" appended to it. This triggers the page to display the Add User Wizard. If the user completes this wizard and clicks the link again to create a third user, the page reloads but the wizard does not appear.

Resolution

Turns out each click of the Create another user link was adding another querystring to the URL, resulting in multiple instances of "action=add" appearing in the URL. This caused the wizard to not appear. The fix was to remove the query string parameter "action" before adding it.

The original javascript:

```
function createAnotherUser()
{
    window.location.search = window.location.search + '&action=add';
}
```

The new javascript:

```
function createAnotherUser()
{
    var qs = removeQSParm(window.location.search, 'action')
    window.location.search = qs + '&action=add';
}

function removeQSParm(url, param)
{
    // Note: Requires param to be after a '&'
    var re = new RegExp('&' + param + '=?.*?(&|$)', 'i');
    if (url.match(re))
        return url.replace(re, '$2');
    else
        return url;
}
```

Defect Details

Defect Id: 211

Project: Gallery Server Pro

Name: ComponentArt objects not disposed during callback on Manage Users page

Date Found: 5/29/2009

Build #: 2.3.3421

Severity: Low Impact

Date Fixed: 5/29/2009

Build # of Fix: 2.3.3436

Status: Closed

Estimated Work: 30 min

Assigned To: Roger Martin

Priority: Low

Actual Work: 30 min

Reported By: Roger Martin

Percent Complete: 100

Description

The ComponentArt Callback control should call dispose on all ComponentArt controls contained within the Callback's template. This is per advice from ComponentArt at <http://www.componentart.com/kb/article.aspx?id=10163>.

This is not being done on the Manage Users page.

No negative behavior was actually observed from this omission, so this is being fixed only because it is recommended.

Resolution

A javascript handler was added to the OnBeforeCallback event on the Manage Users page to call dispose on the TabStrip and MultiPage objects:

```
function cbEditUser_OnBeforeCallback(sender, e)
{
    if (tsEditUser != null)
        tsEditUser.dispose();

    if (mpEditUser != null)
        mpEditUser.dispose();
}
```

Defect Id: 212

Project: Gallery Server Pro

Name: Create User method fails for SQLite when no email is specified (does not affect GSP)

Date Found: 5/28/2009

Build #: 2.3.3421

Severity: No Impact

Date Fixed: 5/29/2009

Build # of Fix: 2.3.3436

Status: Closed

Estimated Work: 30 min

Assigned To: Roger Martin

Priority: Low

Actual Work: 30 min

Reported By: Roger Martin

Percent Complete: 100

Description

NOTE: This is a bug in the SQLite Membership provider, but it was not exposed in Gallery Server Pro, as it never invokes the method with the problem.

When the Membership.CreateUser method is called that has only two parameters (username and password), a null object exception occurs. This is because this method delegates to an overload of this method that calls the ToString() method on the email parameter, which in this scenario is null.

Resolution

Defect Details

The code in the method `MembershipUserCreateUser(stringusername,stringpassword,stringemail,stringpasswordQuestion,stringpasswordAnswer,boolisApproved,objectproviderUserKey,outMembershipCreateStatusstatus)` was changed from this:

```
cmd.Parameters.AddWithValue("$LoweredEmail",email.ToLowerInvariant());
```

to this:

```
cmd.Parameters.AddWithValue("$LoweredEmail", (email !=null? email.ToLowerInvariant() :null));
```

Defect Id: 213

Project: Gallery Server Pro

Name: Hiding the login controls also hides the "My account" button

Date Found: 5/16/2009

Build #: 2.3.3421

Severity: Medium Impact

Date Fixed: 5/29/2009

Build # of Fix: 2.3.3436

Status: Closed

Estimated Work: 1 hrs

Assigned To: Roger Martin

Priority: Medium

Actual Work: 30 min

Reported By: Roger Martin

Percent Complete: 100

Description

If the Show Login option is unchecked on the Site Settings - General page, the "My account" button is also hidden.

Resolution

The button for the My account link was refactored out of the login control (`Website\gs\controls\login.ascx`) and into its own control (`Website\gs\controls\myaccount.ascx`). Logic was added to `galleryheader.ascx` to add this control to the page output when the user is logged in.